Fraud Awareness and Prevention Checklist

Help Protect Your Organization with Active Fraud Prevention and Risk Management
ANTI-FRAUD BEST PRACTICES CHECKLIST

The incidence and severity of fraudulent activity is increasing. As electronic transactions become the norm for all businesses, new forms of fraud arise. It is a permanent reality that businesses must take preventative measures to combat both internal and external fraud in the following areas:

- Computer Best Practices
- Safe Internet Browsing Habits
- Account Structure
- Transaction Protection
- Internal Operations
- Banking Services

**COMPUTER BEST PRACTICES**

☐ Keep operating system software up to date.
☐ Keep other software up to date. Don’t forget programs like Java™, Adobe, and web browsers (Firefox® and Internet Explorer®).
☐ Uninstall programs that are not used or unnecessary.
☐ Implement a firewall.
☐ Install Anti-Virus, Anti-Malware and Anti-Spyware software. Keep these systems up to date, and scan for issues regularly.
☐ Install an Anti-Malware browser plug-in.
☐ Never use the same computer to initiate and approve transactions. Each user should log in from a separate computer.

☐ Ensure your computers are being backed up to protect data in the event of a computer failure.
☐ Use “strong” passwords with at least 8 characters that include a combination of mixed case letters, symbols, and numbers; don’t share passwords; protect passwords; change passwords frequently.
☐ NEVER give your password to anyone, even the help desk.
☐ Use separate passwords for each user accessing bank systems. Never share user IDs among employees.
☐ Never leave your computer unattended; install screensaver timeouts.
☐ Have an incident response plan in place.

**SAFE INTERNET BROWSING HABITS**

☐ Do not install software from unknown sources.
☐ Do not click on web advertisements or ‘pop-ups’.
☐ Do not open attachments on e-mails that you did not expect. Be suspicious of emails purporting to be from a financial institution. Opening file attachments or clicking on web links could expose your system to malicious code that could hijack your computer. Contact the sender to verify it is legitimate before opening the attachment.

☐ If possible, use a dedicated computer for processing bank transactions. Use a separate computer to check email and browse the Internet. Do not use public or unsecured computers.
☐ Only log in as a ‘user’ on the machine. Do not stay logged in as the local administrator.
☐ Delete online user IDs as part of the exit procedure when employees leave your employment.

Learn more about fraud prevention strategies and tools by visiting calbanktrust.com/fraudprevention.
TRANSACTION PROTECTION

- Formalize policy and procedures for the destruction of secure documents.
- Implement policies requiring employees to log off online accounts after they no longer need to be logged in.
- Establish employee transition and termination procedures that include log-in credentials and passwords.
- Maintain ACH and wire transfer limits for both the organization and each user. Establish transaction dollar limits for initiation, approval and release of money transfers.
- Review and reconcile all accounts daily and monthly.
- Adopt a policy to confirm email requests received from other employees to initiate wire transactions, using a known phone number or in person.
- Adopt a policy that all requests for wire transfers or change in wiring instructions sent by email be confirmed in person or over the phone.
- Take advantage of available alerts: balance, transfer, password change, and email address updates.

INTERNAL OPERATIONS

- Use dual authorization for all bank transactions, including wire transfers, online ACH originations, ACH direct transmissions, and remote deposit.
- Use dual control on check issue filing and facsimile signature stamps.
- Restrict, manage & monitor employee access to account information and the ability to move money.
- Promptly remove access for any employee who leaves the company or has a change of responsibility.
- Train staff on controlling access to sensitive information that may be used fraudulently.
- Set policies regarding passwords that include: alphanumeric passwords, different passwords for different applications; change often.
- Separate employees to initiate/approve transactions and audit the monthly bank statement.
- Conduct employee training that helps employees understand fraud prevention Best Practices.
- Have a disaster contingency/data breach plan in place.
- Separate accounts for payroll and operations.

BANKING SERVICES*

- Use Positive Pay to help protect against check fraud.
- Use ACH Positive Pay to help protect against fraudulent ACH debits and electronic payments.
- Use Account Reconciliation services to improve audit control and avoid inefficient manual reconciliation processes.
- Use Automated Clearing House (ACH) to increase efficiency and lower cost by reducing the need to process paper items.
- Use our online banking services (Calbank Network and Direct Business) to obtain critical account information.
- Consider outsourcing receivables processing to California Bank & Trust’s lockbox.
- Utilize duplicate statements and have multiple employees review and reconcile each statement.
- Use event notices to be alerted of account changes/activity.
- Download and install IBM® Security Trusteer Rapport® Software by typing ‘Trusteer’ in the search box on calbanktrust.com. Utilize entry tokens for all users who perform administrative functions or initiate payments.

*Contact your Treasury Management Sales Officer or visit calbanktrust.com/business-banking/treasury-management/ for more information on Treasury Management Banking Services.
For 24-Hour Account Information, call CBT Connect at (800) 400-6080.

For a list of our locations, please visit our website at calbanktrust.com.

To reach the branch or banker nearest you, call (800) 355-0512.